

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-319933

(43)Date of publication of application : 31.10.2002

(51)Int.Cl.

H04L 9/08
H04L 12/18
// H04N 7/167

(21)Application number : 2001-122537

(71)Applicant : SONY CORP

(22)Date of filing : 20.04.2001

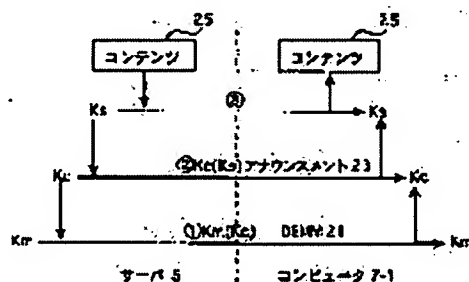
(72)Inventor : TOMINAGA HIROHISA
FUJII NOBORU
TAKEDA TAKASHI
TAKANO AKIYUKI

(54) COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication system, with which contents can be efficiently and safely transmitted from a server side to only a specified client.

SOLUTION: A server 5 and a computer 7-1 hold a master key K_m . The server 5 encrypts a channel key K_c by the master key K_m , places it on a DEMM 21, encrypts a contents key K_s by the channel key K_c , places it on an announcement 23, encrypts and sends contents 25 by the contents key K_s . The computer 7-1 decrypts the DEMM 21 by the master key K_m , acquires the channel key K_c , decrypts the announcement 23 by the channel key K_c , acquires the contents key K_s and decrypts the contents 25 by the contents key K_s .



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

THIS PAGE BLANK (USPTO)

rejection]

[Kind of final disposal of application other than
the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-319933

(P 2 0 0 2 - 3 1 9 9 3 3 A)

(43) 公開日 平成14年10月31日 (2002. 10. 31)

(51) Int. Cl. 7

識別記号

F I

テ-マコード (参考)

H04L 9/08

H04L 12/18

5C064

12/18

9/00

601

B

5J104

// H04N 7/167

601

E

5K030

H04N 7/167

Z

審査請求 未請求 請求項の数22 O L (全8頁)

(21) 出願番号 特願2001-122537 (P 2001-122537)

(22) 出願日 平成13年4月20日 (2001. 4. 20)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 富長 裕久

東京都品川区北品川6丁目7番35号 ソニ

一株式会社内

(72) 発明者 藤井 昇

東京都品川区北品川6丁目7番35号 ソニ

一株式会社内

(74) 代理人 100101557

弁理士 萩原 康司

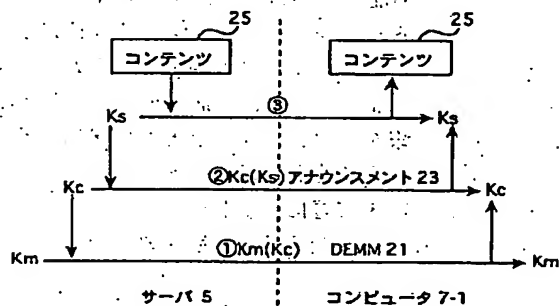
最終頁に続く

(54) 【発明の名称】 通信システム

(57) 【要約】

【課題】 サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供すること。

【解決手段】 サーバ5とコンピュータ7-1は、マスター鍵Kmを保有している。サーバ5は、チャンネル鍵Kcをマスター鍵Kmで暗号化し、DEMM 2-1に載せ、コンテンツ鍵Ksをチャンネル鍵Kcで暗号化し、アナウンスメント23に載せて、コンテンツ2-5をコンテンツ鍵Ksで暗号化して送る。コンピュータ7-1はマスター鍵KmでDEMM 2-1を解読し、チャンネル鍵Kcを取得し、チャンネル鍵Kcでアナウンスメント23を復号化し、コンテンツ鍵Ksを取得し、コンテンツ鍵Ksでコンテンツ2-5を復号化する。



【特許請求の範囲】

【請求項 1】 サーバと端末装置とがネットワークで接続され、マルチキャスト方式で、前記サーバから前記端末装置へコンテンツを配信する通信システムであって、前記サーバは、前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、

前記端末装置は、前記コンテンツ、前記チャンネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする通信システム。

【請求項 2】 前記クライアント情報は、制御情報 D E M M であり、前記チャンネル情報はアナウンスメントであることを特徴とする請求項 1 記載の通信システム。

【請求項 3】 前記サーバと前記端末装置は、マスター鍵を有しており、

前記サーバは、前記マスター鍵でチャンネル鍵を暗号化し、暗号化されたチャンネル鍵をクライアント情報に載せ、前記チャンネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャンネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、前記端末装置は、前記マスター鍵により前記クライアント情報を復号化してチャンネル鍵を得て、このチャンネル鍵で前記チャンネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化することを特徴とする請求項 1 記載の通信システム。

【請求項 4】 前記サーバは、前記チャンネル情報と前記クライアント情報を、コンテンツを送信する通信帯域内で送信することを特徴とする請求項 1 記載の通信システム。

【請求項 5】 前記サーバは、前記チャンネル情報と前記クライアント情報をコンテンツを送信する前に送信することを特徴とする請求項 4 記載の通信システム。

【請求項 6】 前記サーバは、前記チャンネル情報と前記クライアント情報を、コンテンツとともに送信することを特徴とする請求項 4 記載の通信システム。

【請求項 7】 端末装置にネットワークで接続され、マルチキャスト方式で、前記端末装置へコンテンツを配信するサーバであって、

前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送ることを特徴とするサーバ。

【請求項 8】 前記クライアント情報は、制御情報 D E M M であり、前記チャンネル情報はアナウンスメントであることを特徴とする請求項 7 記載のサーバ。

【請求項 9】 マスター鍵を有しており、前記マスター鍵でチャンネル鍵を暗号化し、暗号化されたチャンネル鍵をクライアント情報に載せ、前記チャンネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャンネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送ることを特徴とする請求項 7 記載のサ

ーバ。

【請求項 1 0】 前記チャンネル情報と前記クライアント情報を、コンテンツを送信する通信帯域内で送信することを特徴とする請求項 7 記載のサーバ。

【請求項 1 1】 前記チャンネル情報と前記クライアント情報をコンテンツを送信する前に送信することを特徴とする請求項 1 0 記載のサーバ。

【請求項 1 2】 前記チャンネル情報と前記クライアント情報を、コンテンツとともに送信することを特徴とする請求項 1 0 記載のサーバ。

【請求項 1 3】 サーバとネットワークで接続され、マルチキャスト方式で、前記サーバから配信されるコンテンツを受信する端末装置であって、前記サーバは、前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、前記コンテンツ、前記チャンネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする端末装置。

【請求項 1 4】 前記クライアント情報は、制御情報 D E M M であり、前記チャンネル情報はアナウンスメントであることを特徴とする請求項 1 3 記載の端末装置。

【請求項 1 5】 前記サーバと前記端末装置は、マスター鍵を有しており、

前記サーバは、前記マスター鍵でチャンネル鍵を暗号化し、暗号化されたチャンネル鍵をクライアント情報に載せ、前記チャンネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャンネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、前記マスター鍵により前記クライアント情報を復号化してチャンネル鍵を得て、このチャンネル鍵で前記チャンネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化することを特徴とする請求項 1 3 記載の端末装置。

【請求項 1 6】 前記チャンネル情報と前記クライアント情報をコンテンツを送信する通信帯域内で受信することを特徴とする請求項 1 3 記載の端末装置。

【請求項 1 7】 前記チャンネル情報と前記クライアント情報をコンテンツを送信する前に受信することを特徴とする請求項 1 6 記載の端末装置。

【請求項 1 8】 前記チャンネル情報と前記クライアント情報を、コンテンツとともに受信することを特徴とする請求項 1 6 記載の端末装置。

【請求項 1 9】 請求項 7 から請求項 1 2 までのいずれかに記載されたサーバとしてコンピュータを機能させるプログラム。

【請求項 2 0】 請求項 7 から請求項 1 2 までのいずれかに記載されたサーバとしてコンピュータを機能させるプログラムを記録した記録媒体。

【請求項 2 1】 請求項 1 3 から請求項 1 8 までのい

れかに記載された端末装置としてコンピュータを機能させるプログラム。

【請求項 2 2】 請求項 1 3 から請求項 1 8 までのいずれかに記載された端末装置としてコンピュータを機能させるプログラムを記録した記録媒体。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】本発明は、コンピュータネットワークや、人工衛星を用いたサテライトネットワーク等において、マルチキャスト方式で通信を行う通信システムに関するものである。

【 0 0 0 2 】

【従来の技術】昨今、サーバとクライアントコンピュータとが、インターネット等のコンピュータネットワークや人工衛星を用いたサテライトネットワーク等で接続され、放送と同様にサーバからクライアントにコンテンツ等の配信を行うシステムが実現されつつある。

【 0 0 0 3 】

【発明が解決しようとする課題】ところで、このような通信システムにおいて、限られたクライアントにのみサーバ側からコンテンツを効率的に、かつ安全に送信したいという要望がある。

【 0 0 0 4 】本発明はこのような問題に鑑みてなされたもので、その目的とするところは、サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供することにある。

【 0 0 0 5 】

【課題を解決するための手段】前述した目的を達成するために本発明は、サーバと端末装置とがネットワークで接続され、マルチキャスト方式で、前記サーバから前記端末装置へコンテンツを配信する通信システムであって、前記サーバは、前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、前記端末装置は、前記コンテンツ、前記チャンネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする通信システムである。

【 0 0 0 6 】ここで、サーバとは、コンテンツを配信する機能等を有するコンピュータである。端末装置とは、各家庭等に設置されるようなパーソナルコンピュータ、携帯型端末装置等である。ネットワークとは、通信回路網であり、有線、無線を問わない。ネットワークとしては、例えばインターネット等があり、人工衛星を介したサテライトネットワークも含まれる。

【 0 0 0 7 】マルチキャスト方式とは、端末装置がマルチキャストアドレスを獲得し、このマルチキャストアドレスによってサーバにアクセスし、コンテンツの配信を受ける方式である。このような、マルチキャスト方式では限られた端末装置がコンテンツを受信することができる。コンテンツとは、画像情報や音楽情報等である。ク

ライアント情報とは、制御情報 (D E M M) と称され、コンテンツの配信の対象となるクライアントの I D 等の情報である。

【 0 0 0 8 】チャンネル情報は、アナウンスメントと称され、コンテンツに関する情報である。本発明では、サーバは、コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに端末装置に送り、端末装置は、コンテンツ、チャンネル情報、及びクライアント情報を鍵を用いて所定の順序で復号化する。

【 0 0 0 9 】即ち、前記サーバと前記端末装置は、マスター鍵を有しており、前記サーバは、前記マスター鍵でチャンネル鍵を暗号化し、暗号化されたチャンネル鍵をクライアント情報に載せ、前記チャンネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャンネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送り、前記端末装置は、前記マスター鍵により前記クライアント情報を復号化してチャンネル鍵を得て、このチャンネル鍵で前記チャンネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化する。

【 0 0 1 0 】マスター鍵は、チャンネル鍵を暗号化および復号化する鍵であり、チャンネル鍵は、コンテンツ鍵を暗号化及び復号化する鍵である。コンテンツ鍵は、コンテンツを暗号化及び復号化する鍵である。本発明では、サーバは、前記チャンネル情報と前記クライアント情報とコンテンツを送信する通信帯域内で送信したり、前記チャンネル情報と前記クライアント情報をコンテンツを送信する前に送信したり、前記チャンネル情報と前記クライアント情報を、コンテンツとともに送信する。

【 0 0 1 1 】また、本発明は、端末装置にネットワークで接続され、マルチキャスト方式で、前記端末装置へコンテンツを配信するサーバであって、前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送ることを特徴とするサーバである。

【 0 0 1 2 】即ち、このサーバは、マスター鍵を有しており、前記マスター鍵でチャンネル鍵を暗号化し暗号化されたチャンネル鍵をクライアント情報に載せ、前記チャンネル鍵でコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をチャンネル情報に載せ、前記コンテンツ鍵でコンテンツを暗号化し、前記端末装置に送る。

【 0 0 1 3 】また、本発明は、サーバとネットワークで接続され、マルチキャスト方式で、前記サーバから配信されるコンテンツを受信する端末装置であって、前記サーバは、前記コンテンツ、チャンネル情報及びクライアント情報を夫々暗号化して、鍵とともに前記端末装置に送り、前記コンテンツ、前記チャンネル情報、及び前記クライアント情報を所定の順序で前記鍵を用いて復号化することを特徴とする端末装置である。

【 0 0 1 4 】即ち、この端末装置は、マスター鍵を有し

ており、前記マスター鍵によりサーバから送られるクライアント情報を復号化してチャンネル鍵を得て、このチャンネル鍵でチャンネル情報を復号化してコンテンツ鍵を得て、このコンテンツ鍵で、暗号化されたコンテンツを復号化する。更に、前述したサーバや端末装置としてコンピュータを機能させるプログラムや、このプログラムを記録したCD-ROM等の記録媒体も本発明に含まれる。

【0015】

【発明の実施の形態】以下、図面に基づいて本発明の実施の形態を詳細に説明する。図1は、本発明の実施の形態に係る通信システム1の概略構成図である。この通信システム1はインターネット等のネットワーク3にサーバ5、クライアント側の端末機としてのコンピュータ7-1、7-2、7-3……等が接続されて構成される。

【0016】ネットワーク3は、インターネット等のネットワークであり、有線、無線を含む。尚、ネットワーク3には、人工衛星を介してコンテンツの配信を行うサテライトネットワークも含まれる。サーバ5は、コンテンツの配信等を行う。コンピュータ7-1、7-2……は、例えば一般ユーザの所有するコンピュータである。このコンピュータに代えて携帯型端末機や、電話機能を有する端末機（携帯電話）を用いてもよい。

【0017】次に、この通信システム1の動作について説明する。図2は、サーバ5からコンピュータ7側にコンテンツを配信する場合の説明図である。図2に示すように、サーバ5からコンピュータ7-1等にコンテンツを配信する場合、コンテンツ25の配信と同時に伝送制御情報としてDEMM21とアナウンスメント23を送信する。例えば、午後1時から午後3時の間にコンテンツ25が配信され、このコンテンツ25の配信と同時にDEMM21とアナウンスメント23が配信される。このように、DEMM21とアナウンスメント23は、コンテンツ25を送信する通信帯域内で送信される。

【0018】DEMM(Data Entitlement Management Message)は、クライアント情報である。図3は、DEMM21に搭載される情報を示すもので、DEMM21は、DEMMが暗号化されているかどうかと暗号化の種類を示すフラグ31、クライアントID33、受信許可が与えられているチャンネルID35、コンテンツ鍵Ksが含まれているチャンネル鍵（アナウンスメントの復号鍵）Kc37等を有する。

【0019】DEMMが暗号化されているかどうかと、暗号化の種類を示すフラグ31は、例えばDEMM21が暗号化されているのであれば「1」であり、更に「DES」で暗号化されていれば暗号化の種類を示すフラグ「2」が付加される。クライアントID33は、コンテンツを受信することができるクライアント側のコンピュータ7-1等のID番号である。

【0020】受信許可が与えられているチャンネルID35は、クライアントID33で示されるクライアントが受信できるチャンネルを示すもので、例えばコンピュータ7-1に与えられるチャンネルのID番号である。コンテンツ鍵Ksが含まれているチャンネル鍵Kc37は、クライアント側がアナウンスメント23を解読するための復号鍵である。

【0021】図4は、アナウンスメント23に搭載される情報を示す。アナウンスメント23は、アナウンスメントが暗号化されているかどうかと、暗号化の種類を示すフラグ41、チャンネルを識別する番号（チャンネルID）43、コンテンツを識別する番号（コンテンツID）45、コンテンツが配信されるマルチキャストアドレス47、マルチキャストのポート番号49、コンテンツ鍵Ks51等を有する。

【0022】アナウンスメントが暗号化されているかどうかと、暗号化の種類を示すフラグ41は、例えばアナウンスメントが暗号化されている場合には「1」であり、更に「DES」で暗号化されていれば暗号化の種類を示す「2」が付加される。

【0023】チャンネルID43は、クライアントが利用できるチャンネルを示す。コンテンツID45は、コンテンツ鍵Ks51で復号化されるコンテンツ25のID番号である。マルチキャストアドレス47、マルチキャストのポート番号49は、コンテンツ25が配信されるマルチキャストアドレス及びポート番号である。

【0024】図5、図6は、この通信システム1の処理を示すフローチャートであり、図7は、この通信システム1における鍵情報の伝送手順を示す図、図8はクライアント側の処理を示す図である。以下の例では、クライアントとしてコンピュータ7-1を取り上げて説明する。

【0025】図5に示すように、サーバ5とクライアント側のコンピュータ7-1は、予めマスター鍵Kmを有している（ステップ501、502）。このマスター鍵Kmは、サーバ5及びクライアント側のコンピュータ7-1等にCD-ROM等で送付しておく。または、ネットワーク3を用いて、サーバ5とコンピュータ7-1が、ある共通の数字からマスター鍵Kmを生成するアルゴリズムを保有し、双方でマスター鍵を生成するようにしてもよい。

【0026】サーバ5は、制御情報DEMM21をマスター鍵Kmで暗号化する（ステップ503）。即ち図3に示す制御情報DEMM21が暗号化され、チャンネル鍵Kcもマスター鍵Kmで暗号化され、チャンネル鍵Kc37としてDEMM21に搭載される。サーバ5は、所定のチャンネルのアナウンスメント23をチャンネル鍵Kcで暗号化する（ステップ504）。即ち、図4に示すアナウンスメント23が暗号化され、コンテンツ鍵Ks51もチャンネル鍵Kcで暗号化される。

【0027】更にサーバ5は、コンテンツ25をコンテンツ鍵Ksで暗号化する(ステップ505)。そして、図2に示すように、コンテンツ25をDEMM21、アナウンスメント23とともに送信する(ステップ506)。コンピュータ7-1は、予め保有しているマスター鍵Kmにより、制御情報DEMM21を復号化する(ステップ507)。即ち、図3に示す制御情報DEMM21が復号化され、チャンネルを特定するIDと、そのチャンネルのチャンネル鍵Kc37を取得する(ステップ508)。

【0028】チャンネルを特定するID61は、システム固有のID番号、サーバ5のID番号、チャンネルID番号35等を有する。DEMM21に搭載された情報は次のDEMM21がくるまで、コンピュータ7-1に保存されるが、次のDEMM21を受信した時点ですべて更新する。

【0029】このため、内容が空のDEMM21を受信した場合、クライアントが受信できるコンテンツをなくすことができる。このように、サーバ5がDEMM21の設定を変更すれば、その設定の変更が直ちにクライアント(コンピュータ7-1等)に反映される。

【0030】コンピュータ7-1は、当該チャンネルのアナウンスメント23をチャンネル鍵Kcで解読し、コンテンツ鍵Ks51を取得し、チャンネル情報63を得る(ステップ509)。チャンネル情報63は、チャンネルID43やマルチキャストアドレス47、ポート番号49等である。そして、コンピュータ7-1は、取得されたコンテンツ鍵Ksを用いてコンテンツ25を復号化し、解読する。

【0031】図8は、コンピュータ7-1側の処理を示す説明図である。コンピュータ7-1は、マスター鍵Kmを保有しており、DEMM21をマスター鍵Kmで復号化し、第1チャンネル鍵Kc1、第1チャンネルを特定するID61-1、第2チャンネル鍵Kc2、第2チャンネルを特定するID61-2等を得る。

【0032】コンピュータ7-1は、アナウンスメント23-1を第1チャンネル鍵Kc1で復号化し、チャンネル情報63-1、コンテンツ鍵Ks1を得る。また、コンピュータ7-1は、アナウンスメント23-2を第2チャンネル鍵Kc2で復号化し、チャンネル情報63-2、コンテンツ鍵Ks2を得る。このように、アナウンスメント23-1、23-2は、チャンネルに対応したものである。

【0033】そして、コンピュータ7-1は、コンテンツ25-1をコンテンツ鍵Ks1で復号化し、コンテンツ25-2をコンテンツ鍵Ks2で復号化する。

【0034】このように、本実施の形態によれば、サーバ5は、アナウンスメント23を暗号化することで、チャンネル単位でクライアントのアクセスをコントロールすることができる。また、限られた時間と周波数帯域の中で、DEMM21、アナウンスメント23およびコン

텐츠25を送信することができる。

【0035】そして、コンテンツ25に関する情報をアナウンスメント23に搭載し、クライアントに関する情報をDEMM21に搭載して、DEMM21とアナウンスメント23とを分離して送信するので、全体の制御データ量を減らすことができる。更に、コンテンツ鍵Ks、チャンネル鍵Kc、マスター鍵Kmという三つの鍵を用いて、コンテンツを解読するようにしたので、コンテンツを特定のクライアントにのみ安全に配信することができる。

【0036】更に、コンテンツ鍵Ksをコンテンツごとに変化させた場合でも、アナウンスメント23に含まれる情報を書き換えるだけでクライアント側のコンピュータ7はコンテンツ25の受信が行え、毎回コンテンツ25を送信するごとにマスター鍵Kmを用いて、個別にデータ送信をする必要がないので、コンテンツ25の限定配信を効率的に行うことができる。

【0037】図9、図10は、伝送制御情報の別の送信方式を示すもので、図9では、DEMM21、アナウンスメント23をサーバ5からクライアント側のコンピュータ7に送信した後、コンテンツ25を送信する。DEMM21、アナウンスメント23は、コンテンツの周波数帯域と同じ周波数帯域を用いる。

【0038】図10では、DEMM21、アナウンスメント23を送信した後、コンテンツ25とともにDEMM21、アナウンスメント23を送信する。図9、図10に示す場合は、コンテンツ25の送信開始と同時にすべてのクライアントに受信を開始させることが可能である。

【0039】また、図2、図10の場合、常にクライアントの受信状態を変化させることができる。尚、図2、図10の方式では、コンテンツ25の帯域を圧迫しすぎないように、DEMM21やアナウンスメント23のビットレートの上限値を以下のように定める。

【0040】まず、数値で例えば、100Kbpsのように上限を定める。次に、全体の帯域に対する上限比率を例えば、5%に定める。そして、DEMM21やアナウンスメント23の伝送制御データの送信は、この二つの上限値を超えないようにする。このように上限値を定めることにより、オーバースペックを防ぐことができる。

【0041】

【発明の効果】以上、詳細に説明したように本発明によれば、サーバ側から特定のクライアントにのみコンテンツを効率的に、かつ安全に送信できる通信システムを提供することができる。

【図面の簡単な説明】

【図1】 通信システム1の概略構成図

【図2】 アナウンスメント21とコンテンツ23の送信の説明図

【図 3】 DEMM 21 に搭載される情報を示す図

【図 4】 アナウンスメント 23 に搭載される情報を示す図

【図 5】 通信システム 1 の概略動作を示すフローチャート

【図 6】 通信システム 1 の概略動作を示すフローチャート

【図 7】 通信システム 1 における鍵の伝送手順を示す図

【図 8】 クライアント側のコンピュータ 7 による復号化を示す図

【図 9】 アナウンスメント 21 とコンテンツ 23 の送

信の説明図

【図 10】 アナウンスメント 21 とコンテンツ 23 の送信の説明図

【符号の説明】

1 ……通信システム

3 ……ネットワーク

5 ……サーバ

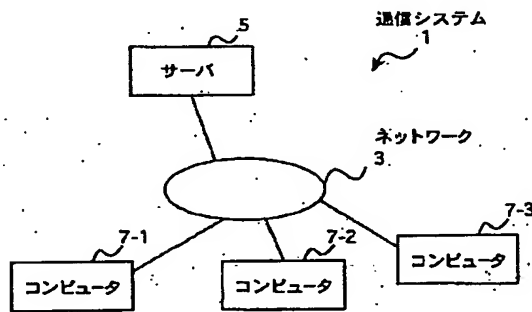
7 ……コンピュータ

21 ……DEMM

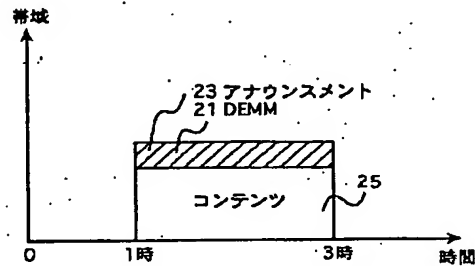
23 ……アナウンスメント

25 ……コンテンツ

【図 1】



【図 2】



【図 3】

21 DEMM

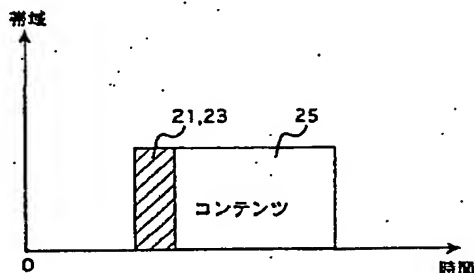
項目	
DEMMが暗号化されているかどうか、暗号化の種類を表すフラグ	31
クライアントID	33
受信許可が与えられているチャンネル ID	35
コンテンツ鍵(Ks)が含まれているチャンネル鍵(Kc)	37

【図 4】

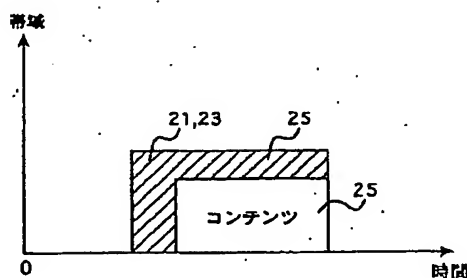
23 アナウンスメント

項目	
アナウンスメントが暗号化されているかどうか、暗号化の種類を表すフラグ	41
チャンネルを識別する番号 (Channel ID)	43
コンテンツを識別する番号 (Content ID)	45
コンテンツが配信されるマルチキャストアドレス	47
マルチキャストのポート番号	49
コンテンツ鍵(Ks)	51

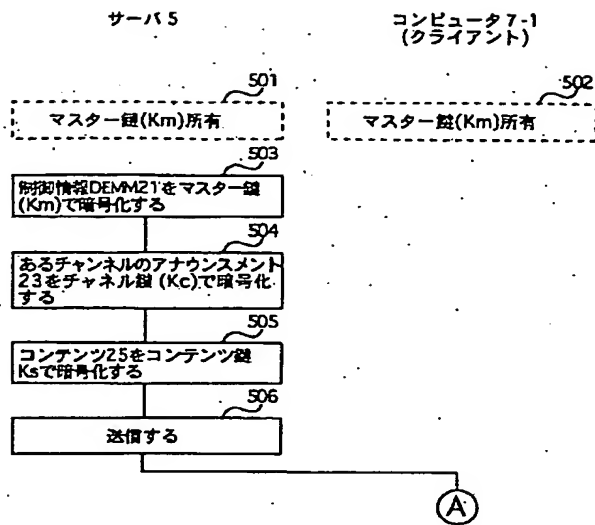
【図 9】



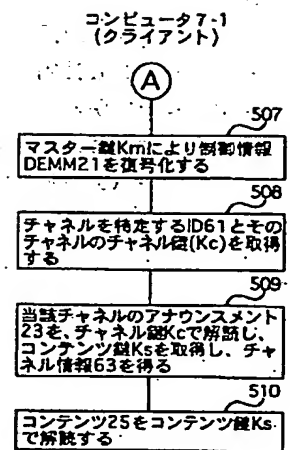
【図 10】



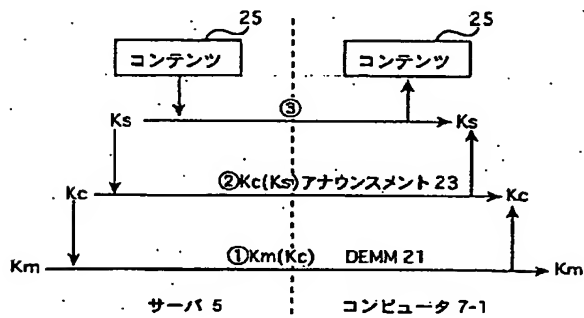
【図5】



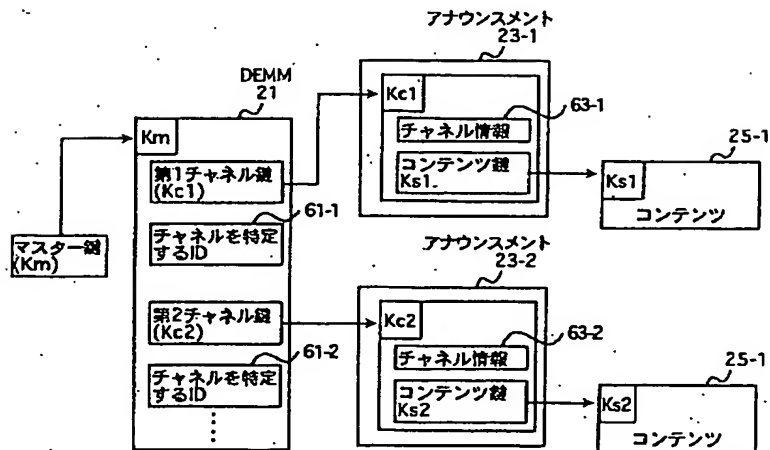
【図6】



【図7】



【図8】





(8)

特開 2002-319933

フロントページの続き

- (72) 発明者 武田 貴志
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内
- (72) 発明者 高野 明幸
東京都品川区北品川 6 丁目 7 番 35 号 ソニ
ー株式会社内

F ターム (参考) 5C064 AA06 AD14 BA07 BB02 BC17
BC22 BD08 BD14 CA14 CA16
CB01 CC01 CC04
5J104 AA16 EA07 EA18 NA02 PA07
5K030 GA15 HB19 KA01 KA02 LD02
LD07